UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/558,138	04/25/2000	Cetin K. Koc	245-53435	9299

7590 12/06/2004

Michael D Jones
Klarquist Sparkman Campbell Leigh & Whinston LLP
121 S W Salmon Street
One World Trade Center Suite 1600
Portland, OR 97204

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/558,138	KOC ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,5,8-10 and 19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,5,8-10 and 19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been presented for examination. Claims 1, 2, 4, 6, 7, 11, 13-17, 19, and 20 have been amended and claims 12, 18, and 21 have been cancelled in an amendment filed 03/04/2004. Claims 3, 5, 8, 10, and 19 have been amended and claims 1, 2, 4, 6, 7, 11, 13-17, and 20 have been canceled in an amendment after final rejection filed 10/14/2004. Claims 3, 5, 8-10, and 19 have been examined.

Docketing

2. This application has been docketed to Primary Examiner Justin T. Darrow in Group Art Unit 2132 in Technology Center 2100.

Response to Amendment

3. The amendment after final rejection filed 10/14/2004 to the claims will be entered in its entirety.

Response to Arguments

4. Applicant's arguments with respect to claims 3, 5, 8-10, and 19 have been considered but are moot in view of the new grounds of rejection.

Claim Objections

5. Claim 3 is objected to because of the following informality: after "$k = k + m$;" delete --and-- in line 9. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 19 is drawn to a computer-readable medium containing instructions for performing a method for computing a multiplicative inverse. A claim drawn to instructions composing a computer program in conjunction with a computer-readable memory is treated as a product claim. See MPEP § 2106 IV. B. 1(a). The instructions in claim 19 result in the performance of a method operating on an M-residue that does not "produce a useful, concrete, and tangible result." See MPEP § 2106 IV. B. 2(a) and *In re Alappat*, 33 F.3d 1526, 1544, 31 USPQ2d 1545, 1557 (Fed. Cir. 1994). The M-residue is just a numerical value not related to any useful information. This can be overcome claiming a message of which the M-residue represents undergoing a transformation. See MPEP § 2106 IV. B. 2(b) i) and *Arrhythmia Research Tech. v. Corazonix Corp.*, 958 F.2d 1053, 1056, 22 USPQ2d 1033, 1036 (Fed. Cir. 1992).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 3, 5, 8, 10, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Shimbo, U.S. Patent No. 6,088,453 A.

As per claim 3, Shimbo describes a computer-readable medium containing instructions for performing a method for transforming a message (see column 1, lines 15-24; information processed in a public key cryptosystem) represented as an element of a complete residue set modulo a prime number *p* into a Montgomery residue of a multiplicative inverse (see column 1, lines 37-56; where information represented in a Montgomery space of integers modulo p), comprising:

selecting a Montgomery radix $R = 2^m$, where *m* is an integer multiple of a wordsize, and *m* is greater than a bit-length of the prime number *p* (see column 8, lines 7-24; R is set to a power of 2 ($R = 2^n$) where it is preferable to set n to be the smallest value that satisfies $n > L$ where L is a number of bits of the modulus p and that is a multiple of the word length);

determining (r, k) from an almost Montgomery inverse function (see column 11, lines 16-35; figure 6, inverse calculation unit 301; Montgomery inverse

$X = (A^{-1} \bullet 2^k \bmod p) \bullet 2^{2n-k} \bmod p$, where (r, k) corresponds to $(A^{-1} \bullet 2^k \bmod p)$);

if k is less than *m*, then assigning r a value obtained as a Montgomery product of *r* and $R^2 \bmod p$, and assigning *k* a value $k = k + m$ (see column 11, lines 27-35; where k is an integer greater than or equal to L and less than or equal to 2L is less than n,

$X = (A^{-1} \bullet 2^k \bmod p) \bullet 2^{2n-k} \bmod p$, where $R = 2^n$ and $k = k + n$);

obtaining the multiplicative inverse as a Montgomery product of *r* and 2^{2m-k} (see column 11, lines 17-25; $X = C \bullet 2^{2n-k} \bmod p$); and

retrieving a stored value of $R^2 \bmod p$ (see column 11, lines 27-35; $C = A^{-1} \bullet 2^k \bmod p$).

As per claim 5, Shimbo discloses a cryptographic system for encryption and decryption comprising a module for transforming a message (see column 1, lines 15-24; information processed in a public key cryptosystem; see column 1, lines 37-56; where information represented in a Montgomery space of integers modulo p; see column 9, lines 62-67; figure 3, item 200; processed in a Montgomery division device), comprising:

representing the message as an element of a complete residue set modulo a prime number *p* (see column 1, lines 37-56; where information represented in a Montgomery space of integers modulo p);

selecting a Montgomery radix $R = 2^m$, where *m* is an integer multiple of a wordsize, and *m* is greater than a bit-length of the prime number p (see column 8, lines 7-24; R is set to a power of 2 ($R = 2^n$) where it is preferable to set n to be the smallest value that satisfies $n > L$ where L is a number of bits of the modulus p and that is a multiple of the word length);

determining (r, k) from an almost Montgomery inverse function (see column 11, lines 16-35; figure 6, inverse calculation unit 301; Montgomery inverse

$X = (A^{-1} \bullet 2^k \bmod p) \bullet 2^{2n-k} \bmod p$, where (r, k) corresponds to $(A^{-1} \bullet 2^k \bmod p)$);

if k is less than *m*, then assigning r a value obtained as a Montgomery product of *r* and $R^2 \bmod p$, and assigning *k* a value $k = k + m$ (see column 11, lines 27-35; where k is an integer greater than or equal to L and less than or equal to 2L is less than n,

$X = (A^{-1} \bullet 2^k \bmod p) \bullet 2^{2n-k} \bmod p$, where $R = 2^n$ and $k = k + n$);

obtaining the multiplicative inverse as a Montgomery product of *r* and 2^{2m-k} (see column 11, lines 17-25; $X = C \bullet 2^{2n-k} \bmod p$); and

representing the transformed message as a Montgomery residue of the multiplicative inverse (see column 8, lines 1-14; information corresponding to element A has a Montgomery inverse a, where $a = A \bullet R^{-1} \bmod p$; column 11, lines 27-35; with inputs C and k, the Montgomery inverse $X = C \bullet 2^{2n-k} \bmod p$).

As per claims 8 and 10, Shimbo presents a cryptographic system comprising an encryption/decryption module that performs and a computer readable medium comprising instructions for performing a method for obtaining a classical inverse of a message (see column 17, lines 4-8; figure 13, items 210 and 301; the Montgomery division device comprising an inverse calculation unit to obtain an inverse of information; see column 1, lines 37-56; where information represented in a Montgomery space of integers modulo p), comprising:

assigning a series of binary digits to the message, where the assigned binary digits represent an element of a residue set modulo a prime number *p* (see column 1, lines 37-56; where information represented in a Montgomery space of integers modulo p);

obtaining values (r, k) by calculating an almost Montgomery inverse function of the representation of the message using a Montgomery radix $R = 2^m$ (see column 17, line 25; figure 13, item 301; $Y = B \bullet A^{-1} \bullet R \bmod p$; see column 8, lines 7-24; R is set to a power of 2 ($R = 2^n$)), where *m* is an integer multiple of a wordsize, and *m* is greater than a bit-length of the prime number p (see column 8, lines 7-24; R is set to a power of 2 ($R = 2^n$) where it is preferable to set n to be the smallest value that satisfies n > L where L is a number of bits of the modulus p and that is a multiple of the word length);

if *k* is greater than *m*, then assigning *r* a value equal to a Montgomery product of *r* and 1, and assigning *k* a value of *k* – *m* (see column 16, lines 46-53; figure 12E, steps S827 and S828; if T > p, p is subtracted from the register T value, where register T contains k and p is n; column 17, lines 25-26; R mod p -> $(R^{-1} R^2) \bmod p$); and

calculating the classical inverse as a Montgomery product of *r* and 2^{m-k} (see column 17, lines 30; $Y = D \bullet 2^{2n-k} \bmod p$, which is equivalent to $D \bullet 2^n \bullet 2^{n-k} \bmod p$).

As per claim 19, Shimbo describes a computer-readable medium containing instructions for performing a method for computing a multiplicative inverse of an M-residue $A = a\ 2^m \bmod p$, where *p* is a prime number, *m* is an integer, and a Montgomery radix $R = 2^m$ (see column 8, lines 7-24; R is set to a power of 2 ($R = 2^n$) where it is preferable to set n to be the smallest value that

satisfies n > L where L is a number of bits of the modulus p and that is a multiple of the word length; see column 1, lines 37-56; in a Montgomery space of integers modulo p), comprising:

computing an intermediate product r and an integer k using an almost Montgomery inverse procedure (see column 17, line 25; figure 13, item 301; $Y = B \bullet A^{-1} \bullet R \bmod p$);

retrieving a value $R^2 \bmod p$ (see column 17, line 26;

$Y = B \bullet (A^{-1} \bullet 2^k)\, 2^{-k} \bullet (R^{-1} \bullet R^2) \bmod p$);

assigning an intermediate product *r'* the value or a Montgomery product of *r* and R^2 (see column 17, line 27; $Y = B \bullet (A^{-1} \bullet 2^k \bmod p) \bullet R^{-1}\ (R^2 \bullet 2^{-k}) \bmod p$); and

obtaining the multiplicative inverse as a Montgomery product *r'* and 2^{2m-k} (see column 17, line 28; $Y = (B \bullet C \bullet R^{-1} \bmod p) \bullet 2^{2n-k} \bmod p$).

Claim Rejections - 35 USC § 103

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shimbo, U.S. Patent No. 6,088,453 A as applied to claim 8 above, and further in view of Kobayashi et al., U.S. Patent No. 6,795,553 B1.

Shimbo discloses the cryptographic system of claim 8. Although he points out that the cryptographic system can be implemented in either hardware or software (see column 17, lines 55-58), he does not explicitly teach an integrated circuit. Kobayashi et al. describes an integrated circuit used in division and multiplication by power of 2 (see column 19, lines 54-59; the multiplication/division by power of 2 is equivalent to the one-bit shift operation, and has the advantage of easy implementation by an electronic circuit or electronic computer). Therefore, it

would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic system of Shimbo with the integrated circuit of Kobayashi et al. for easy implementation (see column 19, lines 54-59).

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an

amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100 thereafter.

December 1, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100